Controls Assessment Checklist

Yes / No	Control	Explanation
No	Least privilege	Everyone within the company has access to all of the internally stored data
No	Disaster recovery plans	No disaster recovery plans in place
No	Password policies	Current policy is not in line with current minimum password complexity requirements
No	Separation of duties	This has not been established
Yes	Firewall	Installed and blocks traffic based on appropriately defined rules
No	Intrusion detection system (IDS)	This has not been installed
No	Backups	There are no backups of critical data
Yes	Antivirus software	This is installed and regularly monitored
No	Manual monitoring, maintenance, and intervention for legacy systems	There is no regular schedule for monitoring and maintenance, methods are also unclear
No	Encryption	Not currently being used for the acceptance, processing, transmission, and storage of sensitive information
No	Password management system	No system in place, sometimes affects productivity when employees are locked out of the system
Yes	Locks (offices, storefront, warehouse)	There are sufficient locks
Yes	Closed-circuit television (CCTV) surveillance	There is an up-to-date system in place
Yes	Fire detection/prevention (fire alarm, sprinkler system, etc)	There is a functioning system

Compliance Checklist

Yes / No	Best practice	Explanation
Payment Card Industry Data Security Standard (PCI DSS)		
No	Only authorized users have access to customers' credit card information	Everyone within the company has access to it as a result of the least privilege control not being in place
No	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment	System is not secured enough
No	Implement data encryption procedures to better secure credit card transaction touchpoints and data	Encryption is not in place, information is transmitted and stored unsecured
No	Adopt secure password management policies	Password complexity requirements are not met
General Data Protection Regulation (GDPR)		
No	EU customers' data is kept private/secured	It is neither private enough nor secured
Yes	There is a plan in place to notify EU customers within 72 hours if their data is compromised/there is a breach	There is an existing plan in place
No	Ensure data is properly classified and inventoried	Data is not stored securely or efficiently access-wise
Yes	Enforce privacy policies, procedures, and processes to properly document and maintain data	This has been developed and enforced within the IT department
System and Organizations Controls (SOC type 1, SOC type 2)		
No	User access policies are established	Least privilege and separation of duties has not been established
No	Sensitive data (PII/SPII) is confidential/private	Everyone within the company has access to it as a result of the least privilege control not being in place
Yes	Data integrity ensures the data is consistent, complete, accurate, and has been validated	Data integrity is active
No	Data is available to individuals authorized to access it	Data is available to ALL individuals within the business, authorized or not

Recommendations

Both controls and compliance require updates to improve the company's security and protect sensitive data. This includes least privilege, separation of duties, encryption, an intrusion detection system, legacy maintenance program, better password complexity requirements and a management system, and disaster recovery plans.